Analysis of SGTR with PMS software failure accident

Liu Lixin, Wang Haitao

(1,2 Shanghai Nuclear Engineering Research & Design Institute CO.,LTD., Shanghai , 200233, China)

Abstract: Digital instrument and control technology has gradually applied in nuclear power plant (NPP), the common cause failure (CCF) due to improper design and/or use may affect the safety of NPP. The purpose of this paper is to analyze the steam generator tube rupture (SGTR) combined with PMS software common cause failure in third-generation passive nuclear power plants. The III generation passive nuclear power plants provide automatic protection measures for SGTR accidents, including reactor shutdown, core makeup tank initiated, passive residual heat removal system heat exchanger action, isolation startup feedwater and chemical volume control system. To further demonstrate the safety of the plant, it is assumed that all of the above protective measures have failed due to a PMS failure, and verify only DAS signals and operator actions can mitigate the accident and bring the plant to a safe steady-state state. The analysis results show that the ruptured SG will not overfill in the whole accident process, the accident consequences are not limited, and the radioactive consequences meet the limit requirements.

Key words: Steam generator tube rupture(SGTR), SG overfill, Single tube double ended, PMS failure, DAS signal

0 overview

Digital instrument and control technology has been increasingly applied in nuclear power plants. Common cause failure caused due to improper design or use may affect the safety of nuclear power plants. To address CCF in digital instrument and control systems, defense measures such as functional decentralization, quality improvement, real-time monitoring, and diversity should be adopted. According to the requirements of NUREG 0800 BTP 7-19 [1], it is necessary to demonstrate the defense-in-depth design capability of the plant after the software CCF of the protection and safety monitoring system (PMS). The diverse actuation system (DAS) set up in the third-generation passive nuclear power plants provides the necessary instrument and control functions to mitigate the consequences of assumed CCFs in the PMS. Overseas nuclear power plants, such as US-APWR and APR1400, have carried out defense-in-depth and diversity (D3) design for the instrument and control system and completed the analysis and verification. This paper takes the steam generator tube rupture (SGTR) event in Chapter 15 of the safety analysis report of the third-generation passive nuclear power plant as an example to analyze the superimposed PMS software CCF and evaluate the mitigation capability of the defense-in-depth system under this accident.

1 Instrument and Control Design Defense-in-Depth Analysis

1.1 PMS System

The PMS is a safety class system that performs reactor emergency shutdown, ESF actuation, and qualified data processing system(QDPS) functions. The PMS equipment that performs ESF actuation functions and reactor emergency shutdown, as well as the related shutdown breakers and sensors, are mostly set up in quadruple redundancy.

About the author: Liu Lixin (1987 -), female, senior engineer, mainly engaged in reactor thermal hydraulic and safety analysis

***Corresponding author**：Liu Lixin，E-mail：liulixin@snerdi.com.cn

The PMS monitors key plant parameters and drives relevant safety functions when abnormalities occur to achieve and maintain the safe shutdown state of the plant. Together with other safety systems, it provides the ability to respond to expected operational events and assumed accidents. The PMS controls the safety class equipment of the plant and also provides equipment class manual control in the main control room and remote shutdown room for safety class equipment with serious consequences. In addition, the PMS system provides safety function monitoring during and after an accident.

1.2 DAS System

The DAS provides necessary instrument and control functions to reduce the risks associated with assumed CCFs in the PMS system. Possible CCFs include software design errors, etc.

The DAS directly receives signals from dedicated sensors. The DAS contains redundant signal processing units and uses different (diverse) equipment and technologies from the PMS. The main DAS signals are detailed in the following table:

Table 1 DAS signals

Protection Function	Monitored Variables
Reactor trip/Turbine trip	Both RCS hot leg high temperature signals simultaneously reach
	Both SG wide range low level signals simultaneously reach
	Pressurizer low level signal
	Manual reactor trip signal
CMT start	Both SG wide range low level signals simultaneously reach
	Pressurizer low level signal
	Manual CMT start signal
RCP shutdown	Both SG wide range low level signals simultaneously reach
	Pressurizer low level signal
	Manual CMT start signal

2 Analysis Methods and Assumptions

A steam generator tube rupture (SGTR) causes primary side coolant to leak into the secondary side of the steam generator. The break leads to a drop in primary pressure and the contamination of the secondary side by the fluid passing through the tubes. The main consequence is a possible radioactive release to the atmosphere through the power operated relief valve (PORV). For SGTR accidents, it is required to meet both acceptance criteria of no overfill of the faulted SG and the radioactive steam release to the atmosphere not exceeding the limit[2]. This paper assumes that all automatic protection measures for mitigating SGTR, including PRHR and CMT activation and isolation of CVS and SFW, fail due to PMS failure. Only DAS signals and operator actions are used to mitigate the accident.

2.1 Analysis Method

After SGTR, radioactive coolant flows into the secondary side through the break, causing an increase in the water level of the faulted SG and an increase in radioactivity in the secondary side. The reactor trip initiated by DAS, PRHR initiated, and SG feedwater isolation require the operator intervention.

The accident is analyzed and calculated using a thermal-hydraulic system program. This program can simulate the PRHR heat exchanger, CMT, and related protection and safety monitoring system trigger logic, as well as simulate the operator action sequence. It can be used to analyze SGTR accidents in advanced pressurized water reactor (PWR) nuclear power plants.

The radioactive N-16 signal is directly sent to data display and processing system (DDS) and is not affected by PMS failure. Therefore, when the PMS system fails, the N-16 signal remains valid, and the operator can determine the occurrence of an SGTR accident based on the N-16 signal and directly execute the "Steam Generator Tube Rupture" emergency operating procedure [3] to mitigate the accident.

According to the design of DAS signals. in the analysis, it is assumed that the reactor

shutdown, main pump coastdown, turbine trip, and CMT activation are initiated by the DAS signal pressurizer low water level. Actions that cannot be automatically initiated by DAS signals (including main feedwater and startup feedwater isolation, pressurizer heaters isolation, CVS isolation, and PRHR activation, etc.) are assumed to be initiated by the operator according to the emergency operating procedure with a certain delay time.

2.2 Assumptions

The assumptions for the SGTR with PMS software failure accident analysis which is different with the DBA condition are as follows[4]:

PRHR and CMT are at nominal capacities; when the pressurizer low water level DAS signal reached, the reactor trip and pump costdown, the turbine trip, and CMT is activated. When the PMS system fails, the main feedwater regulation remains effective. However, in the analysis, it is conservatively assumed that the main feedwater is continuously supplied at a constant nominal flow rate before the reactor trip. According to the emergency operating procedures, the operator needs to isolate the main feedwater and startup feedwater of the faulted SG and supply the startup feedwater to the intact SG.

In the analysis, it is conservatively assumed that the operator isolates all main feedwater 30 minutes after the accident and simultaneously supplies a constant nominal flow rate of startup feedwater to both loops. Later, the operator isolates the startup feedwater according to the emergency operating procedures. The operator can manually operate the CVS charging pump to maintain the pressurizer level according to the emergency operating procedures. Therefore, in the analysis, it is conservatively assumed that the CVS injects at the maximum injection flow rate at the beginning of the accident. According to the emergency operating procedures, the operator needs to manually start the PRHR. In the analysis, it is conservatively assumed that the operator manually starts the PRHR 10 minutes after manually isolating the pressurizer heater.

3 Results Analysis

At zero time, the double-end break of a single SG tube occurred. The operator manually activated the CVS to provide makeup water flow, and at the same time, the pressurizer heaters were put into operation. The break led to the leakage of reactor coolant from the primary side to the secondary side (as shown in Figure 1), causing the temperature and pressure of the primary side of the reactor coolant system to drop, and the water level in the pressurizer to decrease. When the DAS signal pressurizer low water level reached, the reactor tripped and the pumps stopped, the turbine tripped and the CMT was activated. After the reactor tripped, the pressurizer water level and the primary side pressure dropped rapidly (as shown in Figures 2 and 3), and the water volume in the steam generator increased rapidly (as shown in Figure 4), causing the pressure on the secondary side of the steam generator to rise rapidly (as shown in Figure 5), until it reached the opening pressure of the PORV and opened the valve to release steam.

According to the emergency operating procedures, the operator needs to isolate the main feedwater and startup feedwater of the faulted SG and supply startup feedwater to the intact SG. In the analysis, it is conservatively assumed that the operator isolated all the main feedwater 30 minutes after the accident and simultaneously supplied a constant startup feedwater flow to both loops. According to the pressurizer empty time, it is conservatively assumed that the operator manually isolated the pressurizer heaters 10 minutes after manually isolating the main feedwater, and according to the procedures, the operator needs to activate the PRHR to remove heat. In the analysis, it is conservatively assumed that the operator manually activated the PRHR 10 minutes after

manually isolating the pressurizer heaters.

The break flow caused the water level on the secondary side of the SG to continuously rise. According to the emergency operating procedures, when the narrow range high liquid level of any SG is reached, the CVS isolation valves and the startup feedwater isolation valve should be closed respectively. In the analysis, it is conservatively assumed that the operator delayed 30 minutes to isolate the CVS and startup feedwater after the faulted SG reached the narrow range high liquid level setpoint. After the PRHR operated, the temperature and pressure on the primary side of the RCS dropped rapidly, and the water level in the pressurizer continued to drop. The pressure difference between the primary and secondary sides gradually decreased, causing the break flow to gradually approach to zero (as shown in Figure 1), and the water volume in the steam generator also began to gradually stabilize (as shown in Figure 4). Finally, the pressure on the primary and secondary sides of the steam generator basically reached equilibrium, and the break flow terminated.

Table 2 SGTR with PMS software common cause failure accident sequence

Event	Time（s）
Double-ended break of steam generator tubes	0.0
Pressurizer low water level signal (DAS signal)	1377.0
Reactor trip（DAS signal）	1379.0
CMT initiated (DAS signal)	1389.0
Main feedwater isolation and Startup feedwater operated (operator action)	1800.0
PRHR is put into operation (operator action)	3000.0
Isolation of the charging flow of CVS (operator action)	4723.1
Isolation of startup feedwater (operator action)	4723.1
Break flow terminates	13869.1

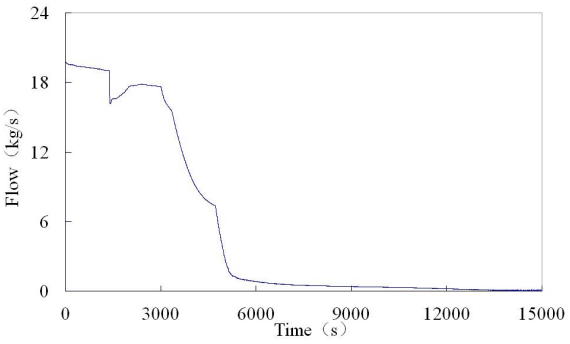

Fig. 1 Break Flowrate

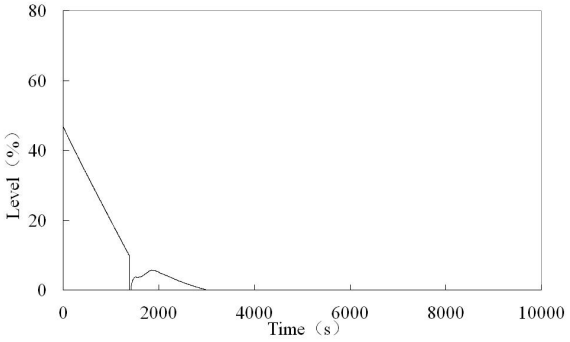

Fig. 2 Pressurizer Level

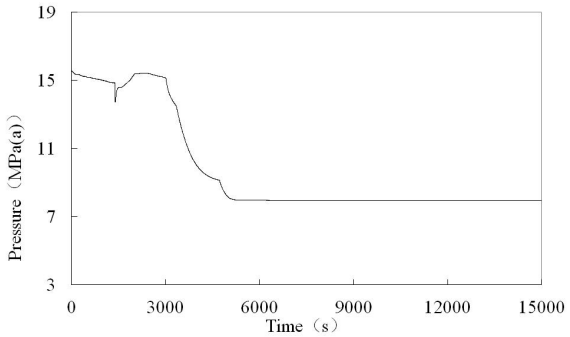

Fig. 3 Pressurizer Pressure

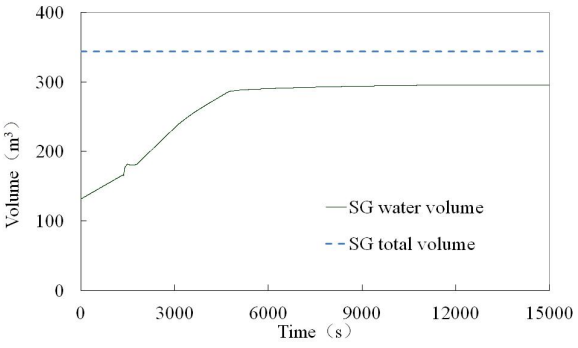

Fig. 4 Faulted SG Water Volume

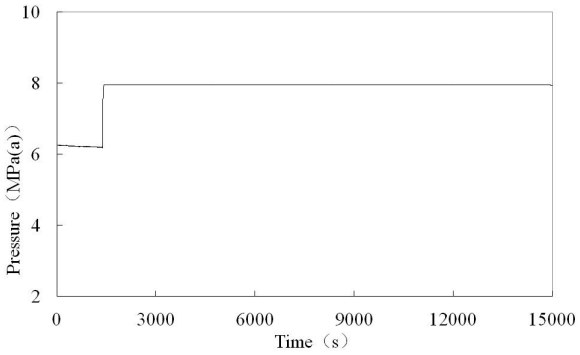

Fig. 5 SG Steam Pressure

4 Conclusion

(1) The SGTR with PMS software failure accident can be effectively mitigated through DAS signals and operator manual intervention. During the accident, the maximum water volume of the SG is 295.8 m³, and the SG overfill margin is 48.0 m³. Throughout the accident, the faulted SG will not overfill, and the accident consequence is not limit. Therefore, the radioactive consequence must also meet the limit requirements.

(2) This is the first time to analyze the SGTR with PMS software failure accident, and only by relying on DAS signals and operator actions to mitigate the accident, which further verifies that the nuclear power plant has the ability to mitigate common cause failure situations, making the SGTR analysis more comprehensive and the accident analysis system more complete.

(3) The analysis further proves that the current third-generation passive nuclear power plant design has the ability to cope with more severe accidents than the design basis accident, including multiple common cause failures, further verifying the safety of the nuclear power plant.

References：

[1] Anon.Final revision to branch technical position 7-19 guidance for evaluation of defense in depth and diversity to address common-cause failure due to latent design defects in digital safety systems[J].The Federal Register / FIND,2021,86(18):7577.

[2] Liu Lixin, Liu Zhan. Extended research on SGTR accident SG overflow analysis [J]. Nuclear Power Engineering, 2020, 41(3): 81-85.

[3] Liu Lixin, Wang Zhe. Research on optimization of SGTR procedures in nuclear power plants [J]. Nuclear Power Engineering, 2022, 43(4): 126-130.

[4] Ke Xiao. Research on SGTR accident in full power range of CAP1000 nuclear power plant [J]. Atomic Energy Science and Technology, 2014, 48(6): 1031-1037.